CyberSecurity Collaboration Summit - 20 Nov - San Diego, CA

A heads up on the CyberSecurity Collaboration Summit we've arranged for Thursday, 20 November here in SD at the Hyatt (see enclosed link for details and registration info). The date and place follow that of MILCOM 2008 to leverage folks travel and time.

The proverbial bottom line - While the agenda and rationale are enclosed below, the reason that WE, the industry's commercial, government and academia partners, must collaborate is that to be maximally effective in this complex and resource constrained IT/IA/Security environment, we all must have a common end-state IA/Security focus and gain consensus on "what really matters in IA?" and the issues that entails, as well as the affordability aspect. Otherwise we will continue to do things just different enough to make integration, interoperability and IA/Security almost
impossible to manage.

http://www.igouge.com <http://www.igouge.com>

Cybersecurity Collaboration Summit
"How do you know a good information assurance ROI when you see one?"

Overall objective - IA/security consortium that helps define the essence of what we need to focus on technically in the Navy / DOD in IA / security...
and any related factors from IS/IO/CNO/etc.

Then identify key gaps and technologies and capabilities we ALL collectively need to get there.

Rationale: Provide a balanced, non-parochial, technical "purist"
perspective, not inhibited by the sponsors inability to pay (at least in the current approach), or any not-invented-here perspectives, or by the fog and confusion of the complexity of it all - so we'll consider the following
topics:

- What is our IA / security vision - based on what formal requirements?
- Top IA/security issues - what really matters?
- Current novel / disruptive initiatives (focus on significant added capability AND less complexity AND lower TOC) (major sponsors and innovators will provide their perspectives).

That is, what sort of technologies and methods can we leverage an implement affordable, such as: dynamic digital policy implementation, game theory to
model and predict cyber attacks and defenses; self-organizing,
self-healing and self-optimizing networks; smart agents and zero knowledge
protocols, and SOA security (what is that anyway?).

- Lessons learned from Estonia (invited - more to follow)
- What is a "best value" in IA anyway... (aka how to measure IA/security) Given we can get an achievable vision, and can effectively measure it - what are our best ROI potentials? What gets us the highest risk reduction in the most critical impact areas that is affordable / implementable?

- Educating leadership - What notional IA/security end-state that we all need to collectively get "them" to champion and what key capabilities should we demand that we all MUST pursue? (as well as follow on actions / recap of the summit)

The full agenda will be developed over the next two weeks of early October.
We have invited key Navy/USMC vendors including McAfee, Symantec, Juniper, Verizon, GuardianEdge along with key integrators like Raytheon and Boeing (a current sponsor)

Members of AFCEA and NDIA will also be invited. This seminar is taking place in San Diego the day after MILCOM 2008 at the San Diego Hyatt.